UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

Eleanor Murray, *on behalf of herself and all others similarly situated,* *Plaintiff,* **v.** Community Care Physicians, P.C., and BST & Co. CPAs, LLP, *Defendants,*	)	Case No.: 1:20-cv-661 (MAD/DJS) **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff ELEANOR MURRAY ("Plaintiff"), individually and on behalf of all others similarly situated, complains and alleges as follows based on personal knowledge as to herself, on the investigation of her counsel, and on information and belief as to all other matters:

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Community Care Physicians, P.C. ("CCP") and its accountants at BST & Co. CPAs, LLP ("BST"), arising from their collective failure to safeguard certain Personally Identifying Information[1] and Protected Health

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the breach.

Information[2] (collectively "PII") of thousands of CCP's current and former patients. Consequently, those patients' PII—including their "name, date of birth, billing code, insurance description (A definition of the billing / CPT code), and medical record number…"—has been compromised.[3]

2. From December 4, 2019 to December 7, 2019, cybercriminals gained access to BST's information technology systems which contained private and confidential PII, including the "names, dates of birth, medical record numbers,

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq*., and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A "covered entity" is further defined as, *inter alia*, a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. *Id. Covered entity*. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). CCP is clearly a "covered entity" and some of the data compromised in the Data Breach that this action arises out of is "protected health information", subject to HIPAA. Moreover, a "business associate" includes an entity that, *inter alia*, provides accounting services to or for a covered entity where the provision of the service involves the disclosure of protected health information from such covered entity, or from another business associate of such covered entity, to that accountant. *Id. Business Associate*. BST, as CCP's accountant, is clearly one of CCP's "business associate[s]", and is therefore also subject to HIPAA.

[3] *Information about BST Security Incident Involving CCP Data*, COMMUNITY CARE PHYSICIANS, P.C., https://www.communitycare.com/News/Articles/Information-about-BST-Security-Incident-Involving-CCP-Data (last accessed June 4, 2020).

medical billing codes, and insurance descriptions…" for 170,000 individuals[4], including patients of CCP (the "Data Breach")[5].

3. As will be more fully explained below, Plaintiff and members of the Class have been significantly injured by the Data Breach and have incurred out-of-pocket expenses associated with the reasonable mitigation measures they were forced to employ. Plaintiff and the Class also now forever face an amplified risk of fraud and identity theft due to their sensitive PII falling into the hands of cybercriminals.

4. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action sounding in negligence, breach of contract, including breach of the covenant of good faith and fair dealing, trespass to chattels, bailment, violation of N.Y. GBL § 349, *et seq*. unjust enrichment, and conversion. Plaintiff seeks damages and injunctive and declaratory relief arising from CCP's failure to adequately protect her highly sensitive PII.

PARTIES

5. Plaintiff Eleanor Murray is a natural person who resides in Niskayuna, County of Schenectady, State of New York. Mrs. Murray is a current patient of CCP.

---

[4] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed June 4, 2020).
[5] *BST & Co. CPAs, LLP Provides Notice of Data Privacy Event*, BST & CO. CPAS, LLP, https://www.bstco.com/notice-of-data-privacy-event/ (last accessed June 4, 2020).

6. Defendant Community Care Physicians, P.C. is a domestic professional corporation organized under the laws of Delaware with its principal office located at Capital Region Health Park 711 Troy-Schenectady Road Suite 201 Latham, New York 12110.

7. CCP is a large, independent multispecialty medical group in the Capital Region of New York, with more than 2,000 employees, including more than 420 practitioners, across 80 locations, and 30 specialties in 8 counties of the greater Capital Region of New York.

8. Defendant BST & Co. CPAs, LLP is a limited liability partnership organized under the laws of Delaware with its principal office located at 26 Computer Drive West Albany, New York 12205.

9. BST is a multi-disciplinary accounting, tax and advisory firm which has many clients across the area, including CCP. CCP uses BST for accounting services.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because: (i) there are more than 100 Class Members; (ii) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest and costs; and (iii) upon information and belief, some Class Members are citizens of states different than CCP and BST's home state of New York.

11. This Court has personal jurisdiction over CCP because it maintains a principal place of business in this judicial district and regularly conducts business in New York.

12. This Court likewise has personal jurisdiction over BST because it also maintains a principal place of business in this judicial district and regularly conducts business in New York.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because CCP and BST reside in this district and regularly conduct business in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and CCP and BST have caused harm to Class Members residing in this district.

FACTUAL ALLEGATIONS

A. Plaintiff and the Class Members entrusted their PII to CCP

14. Plaintiff and the members of the Class are present and former patients of CCP.

15. As a condition for receiving treatment, Plaintiff and Class members were required by CCP to confide and make available to it, its agents, and its employees, sensitive and confidential PII, including, but not limited to, their names, dates of birth, addresses, health insurance information, and other clinical and treatment information related to the care sought there.

16. CCP acquired, collected, and stored a massive amount of PII of its patients.

17. By obtaining, collecting, using, and deriving a benefit from its patients' PII, CCP assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their PII from unauthorized disclosure.

18. Plaintiff has taken reasonable steps to maintain the confidentiality of her PII. Plaintiff, as a current and former patient, relied on CCP to keep her PII confidential and securely maintained, to use this information for business purposes only, and to take reasonable steps to ensure that its vendors would make only authorized disclosures of this information.

19. Indeed, CCP maintains a policy which specifically acknowledges its legal obligation to maintain the privacy of patient PII entrusted to it and to control the disclosure thereof.

20. CCP's policy is outlined in its Notice of Privacy Practices (CCP's "Privacy Policy"), which was effective on April 14, 2003, and was last revised on June 1, 2013.[6]

21. In its Privacy Policy, CCP represents that it is "dedicated to maintaining the privacy of [patients'] individually identifiable health information."[7] CCP's Privacy Policy goes on to circumscribe the way patients' PII can and cannot be disclosed to, *inter alia*, third parties.[8] The Privacy Policy represents that CCP is

---

[6] *Community Care Physicians, P.C. Notice of Privacy Practices*, COMMUNITY CARE PHYSICIANS, P.C., https://www.communitycare.com/Notice-Of-Privacy-Practices (last accessed June 4, 2020).
[7] *Ibid.*
[8] *Ibid.*

"required by law to maintain the confidentiality of health information that identifies [patients]."[9] The Data Breach that is the subject of this civil action is not contemplated or permitted by CCP's Privacy Policy.[10]

22. Plaintiff entrusted her PII to CCP solely for the purpose of effectuating treatment and the payment therefor with the expectation and implied mutual understanding that CCP would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

23. Plaintiff would not have entrusted CCP with her highly sensitive PII if she had known that CCP would entrust it to a vulnerable vendor, such as BST, thereby failing to protect it from unauthorized use or disclosure.

B. The security of patients' PII was compromised in the Data Breach

24. Plaintiff has been a patient of CCP for years.

25. When Plaintiff presented herself to CCP for treatment, its agents prominently posted and/or provided Plaintiff with various disclosure statements regarding CCP's Privacy Policy and its obligations under HIPAA to safeguard patients' PII–as CCP was required to do by law.[11]

26. As a prerequisite to receiving treatment, Plaintiff divulged her personal and sensitive PII to CCP, with the implicit understanding that her PII

---

[9] *Ibid.*
[10] *Ibid.*
[11] *See, e.g.*, 45 C.F.R. § 164.520(c)(2)(iii)(B).

would be kept confidential. This understanding was based on all the facts and circumstances attendant to her receiving care, and the express, specific, written representations made by CCP and its agents.

27. Plaintiff reasonably relied upon CCP's representations to her detriment and would not have provided her sensitive PII to CCP if not for CCP's explicit and implicit promises to adequately safeguard that information.

28. CCP entrusted the PII that is at issue in this action to BST in order to use its accounting services.

29. According to CCP, on or around December 4, 2019, one or more wrongdoers obtained access to BST's information technology systems and stole private and confidential PII, including CCP's patients' "name[s], date[s] of birth, billing codes, insurance description[s] (A definition of the billing / CPT code), and medical record number[s]."[12]

30. According to CCP, "there was an unauthorized intrusion into BST's network that contained Community Care Physicians' data… by an unknown individual or individuals outside of BST who gained access to part of the network where certain client files are stored, including files from CCP…" by way of a ransomware virus.[13]

31. CCP urged those affected by the Data Breach to "remain alert to potential misuses of your personal information and we recommend you take

[12] *Ibid.*
[13] *Ibid.*

proactive steps to protect yourself from any unwanted use of your information that may occur as a result of this incident…"[14]

32. Per CCP's notification, cybercriminals had uninhibited access to Plaintiff's and Class Members' PII for nearly four days.

33. As a result of this Data Breach, the PII of 170,000 individuals whose PII was in the possession of BST was compromised.

34. The Data Breach was preventable and a direct result of BST's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' PII.

35. The Data Breach was moreover a direct result of CCP entrusting the Plaintiff's PII to BST without conducting reasonable inquiry into BST's data security practices.

36. Further, BST allegedly discovered the breach on December 7, 2019, but Plaintiff and the Class were not notified for months, on or about February 14, 2020.

37. On or about February 14, 2020, CCP sent letters to the Class members notifying them that their PII had been compromised during the Data Breach.[15]

C. The healthcare industry is a prime target for cybercriminals

38. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a

[14] *Ibid.*

[15] *Information about BST Security Incident Involving CCP Data, supra* note 3.

40% increase from 2015.[16] The next year, that number increased by nearly 50%.[17] The following year the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[18]

39. Data breaches within the healthcare industry in general, and with vendors in particular, continued to rapidly increase. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68 percent of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[19]

40. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of

---

[16] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/.

[17] *2017 Annual Data Breach Year-End Review*, ITRC, (Jan. 25, 2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

[18] *2018 End-of-Year Data Breach Report*, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[19] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[20]

41. The PII stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach— most notably name and date of birth —is difficult, if not impossible, to change.

42. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[21] Likewise, the FBI has warned healthcare organizations that PII data is worth 10 times as much as personal credit card data on the black market.[22]

---

[20] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH, (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[22] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. *See* Humer, Caroline & Finkle, Jim, *Your medical record is worth more to hackers than your credit card*, REUTERS, (Sep. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924. Dark web monitoring is a commercially available service which, at a minimum, BST can and should perform (or hire a third-party expert to perform).

43. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers.

44. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

45. As storehouses of that lucrative information, business associates like BST are also highly targeted by cybercriminals because they lack "sufficient resources to prevent or quickly detect a data breach" making them an easier target.[23]

46. Cybercriminals regularly target the healthcare industry with email phishing schemes, which "remain[] the primary attack vector for nine out of 10 cyberattacks."[24] CCP did not elaborate on how the Data Breach happened, other than a description that suggests it was a ransomware attack.[25] Since "91% of

---

[23] *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*, PONEMON INSTITUTE LLC 40 (May 11, 2016), https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf (according to survey participants, a mere 41% of business associates reported that they felt they had sufficient resources to combat threats in 2015, and that number only increased to 48% in 2016).

[24] Benishti, *supra* note 20.

[25] *See Information about BST Security Incident Involving CCP Data*, *supra* note 3.

ransomware attacks are the result of phishing exploits…" in the healthcare sector, it is more than plausible that the Data Breach was due to a phishing attack too.[26]

47. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

48. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PII.

49. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

[26] *Security Report Health Care – Hospitals, Providers and more*, CORVUS INSURANCE 2 (Mar. 3, 2020), https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf.

D. CCP failed to sufficiently protect the PII that patients had entrusted to it, and BST failed to sufficiently protect the PII that CCP entrusted to it

i. CCP and BST failed to adhere to HIPAA

50. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[27]

51. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII is properly maintained.[28]

52. Moreover, since CCP is a covered entity, and BST is its business associate, HIPAA requires that CCP, *inter alia*, obtain satisfactory assurances from BST that it will appropriately safeguard the PII it receives or creates on behalf of CCP.[29]

---

[27] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, social security numbers and medical record numbers.

[28] *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

[29] *See* 45 C.F.R. § 164.502(e)(1)(i).

53. The Data Breach itself resulted from a combination of inadequacies showing BST failed to comply with safeguards mandated by HIPAA. BST's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by BST's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

ii. CCP and BST failed to adhere to FTC guidelines

54. According to the Federal Trade Commission("FTC"), the need for data security should be factored into all business decision-making.[30] To that end, the

[30] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

FTC has issued numerous guidelines identifying best data security practices that businesses, such as CCP and BST, should employ to protect against the unlawful exposure of PII.

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[31] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

56. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for

[31] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. CCP and BST's collective failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

59. Moreover, BST is required to comply with the Safeguards Rule of the Gramm-Leach-Bliley Act, which requires it to, *inter alia*:

a. Designate one or more employees to coordinate its information security program;

b. Identify and assess the risks to client information in each relevant area of the firm's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;

c. Design and implement a safeguards program, and regularly monitor and test it;

[32] *See Start with Security, supra* note 30.

d. Select service providers that can maintain appropriate safeguards, making sure their contracts require them to maintain these safeguards; and

e. Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

60. BST's failure to adhere to the Safeguards Rule certainly contributed to the Data Breach.

iii. CCP failed to adhere to industry standards

61. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[33] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record.[34] As a result, both the government and private sector have developed industry best standards to address this growing problem.

62. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain

[33] 2018 End of Year Data Brach Report, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/ wp-content/uploads/2019/02/ITRC_2018-End-of-Year Aftermath_FINAL_V2_ combinedWEB.pdf.
[34] *Ibid.*

access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[35] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[36] Most notably, organizations must properly encrypt PII in order to mitigate against misuse.

63. The private sector has similarly identified the healthcare sector as particularly vulnerable to cyber-attacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[37]

64. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, BST failed to adopt sufficient data security processes – and CCP failed to ensure that BST implemented those processes – a fact highlighted in CCP's notification to affected patients in which it revealed that only after the Data Breach was BST "taking steps to

---

[35] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

[36] *Ibid.*

[37] *10 Cyber Security Best Practices For the Healthcare Industry*, NTIVA (Jun. 19, 2018), https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry.

minimize the potential for unauthorized access to their environment and making reasonable efforts to ensure the continued security of [patients'] information."[38]

65. CCP failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining and communicating sensitive data.

66. BST's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

E. Plaintiff and the Class Members were significantly harmed by the Data Breach

67. As discussed above, PII is among the most sensitive, and personally damaging information. A report focusing on breaches in the healthcare industry

[38] *Information about BST Security Incident Involving CCP Data, supra* note 3.

found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000.00" per person, and that the victims were further routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[39]

68. Victims of medical identity theft can suffer significant financial consequences. "In some cases, they [must pay] the healthcare provider, repa[y] the insurer for services obtained by the thief, or . . . engage[] an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[40]

69. Moreover, nearly half of identity theft victims lost their health care coverage as a result of a data breach incident, nearly one-third reported that their premiums went up, and forty percent never resolved their identity theft at all.[41]

70. "Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful and expensive to resolve."[42]

---

[39] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[40] *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE LLC 1 (Nov. 18, 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65.
[41] *Ibid.*
[42] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN (Apr. 13, 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

71. Moreover, resolution of medical identity theft is time consuming to remedy. "Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident."[43] Consequently, they remain at "risk for further theft or errors in [their] healthcare records that could jeopardize medical treatments and diagnosis."[44]

72. As a result of the Data Breach, Plaintiff now faces, and will continue to face, a heightened risk of identity theft and fraud for the rest of her life.

73. As a long-standing member of the healthcare community, CCP knew or should have known the importance of safeguarding patient PII entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, CCP failed to ensure that its business associate BST took adequate cyber-security measures to prevent the ransomware attack from happening.

74. Neither CCP nor BST have provided any compensation to patients victimized in the Data Breach or have offered to provide any assistance or compensation for the costs and burdens — current and future — associated with the identity theft and fraud resulting from the Data Breach.

75. Even if CCP and BST did reimburse Plaintiff for the harm she suffered, it is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary,

---

[43] *Ibid.*
[44] *Ibid.*

after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[45]

76. As a result of CCP and BST's collective failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer significant damages. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise, publication and/or theft of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

e. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

[45] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

researching how to prevent, detect, contest and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII;

h. The continued risk to their PII, which remains in the possession of CCP and BST and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII in their possession; and

i. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

77. Plaintiff has already incurred harms as a result of the Data Breach.

78. For example, in an effort to mitigate the heightened risk of identity theft and fraud that they now face, Plaintiff has subscribed to Equifax Gold Shield, which provides her with online credit scores to consumers direct from the credit bureaus. While this credit monitoring service allows Plaintiff to monitor her credit reports to determine whether suspicious activity has occurred, it is powerless to stop identity theft in advance and the indemnification and insurance it provides is subject to conditions and exclusions, it will not eliminate the harm caused by the Data Breach.

79. In addition to the out-of-pocket expenses Plaintiff has incurred relating to the reasonable mitigation efforts that they have employed; Plaintiff has also expended time and effort in order to mitigate the harm she has suffered on account of the Data Breach.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Fed. R. Civ. Proc. 23. The Class is preliminarily defined as:

> All individuals whose PII was compromised as a result of the Data Breach with BST & Co. CPAs, LLP which was announced by Community Care Physicians, P.C. on February 19, 2020.

81. Excluded from the Class are CCP, BST and their subsidiaries and affiliates, their officers, directors and member of their immediate families and any entity in which they have a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

82. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or to add a subclass(es) if necessary, before this Court determines whether certification is appropriate.

83. *Fed. R. Civ. P. 23(a)(1) Numerosity:* The Class is so numerous such that joinder of all members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of 170,000 current and former patients of CCP, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to CCP and BST's records. CCP and BST have the

administrative capability through their computer systems and other records to identify all members of the Class, and such specific information is not otherwise available to Plaintiff.

84. *Fed. R. Civ. P. 23(a)(2) Commonality and Fed. R. Civ. P. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the members of the Class. These questions predominate over questions that may affect only individual members of the Class because CCP and BST have acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether CCP and BST had a duty to protect patient PII;

b. Whether CCP and BST knew or should have known of the susceptibility of BST's systems to a data breach;

c. Whether BST's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether CCP and BST were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether CCP and BST's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether CCP or BST's conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach,

resulting in the unlawful exposure of the Plaintiff's and Class members' PII;

g. Whether Plaintiff and Class members were injured and suffered damages or other losses because of CCP and BST's failure to reasonably protect BST's systems and data network;

h. Whether Plaintiff and Class members are entitled to relief;

i. Whether CCP failed to adequately notify Class members of the compromise of their PII;

j. Whether CCP assumed a fiduciary duty and/or confidential relationship to Class members when they entrusted it with their PII;

k. Whether CCP breached its contracts with Class members by failing to properly safeguard their PII and by failing to notify them of the Data Breach;

l. Whether CCP and BST's violation of HIPAA constitutes evidence of negligence; and

m. Whether CCP impliedly warranted to Class members that the information technology systems of its business associates were fit for the purpose intended, namely the safe and secure processing of PII, and whether such warranty was breached.

85. *Fed. R. Civ. P. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims of all Class members, because all such claims arise from the same set of facts

regarding CCP and BST's collective failure:

a. to protect Plaintiff's and Class members' PII;

b. to discover and remediate the security breach of BST's computer systems more quickly; and

c. to disclose to Plaintiff's and Class members in a complete and timely manner information concerning the security breach and the theft of their PII.

86. *Fed. R. Civ. P. 23(a)(4) Adequacy:* Plaintiff' will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff is a victim of the Data Breach, have incurred reasonable mitigation damages as a result of the Data Breach, and bring the same claims on behalf of herself and the putative Class. Plaintiff has no interests antagonistic to that of the Class member. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

87. *Fed. R. Civ. P. 23(b)(2) Injunctive and Declaratory Relief:* CCP and BST have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

88. *Fed. R. Civ. P. 23(b)(3) Superiority:* It is impracticable to bring Class

members' individual claims before the Court. Class treatment permits a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

89. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

a. The unnamed members of the Class are unlikely to have an interest in individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is desirable;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

90. Plaintiff knows of no unique difficulty to be encountered in the

prosecution of this action that would preclude its maintenance as a class action.

91. *Fed. R. Civ. P. 23(c)(4) Issue Certification:* Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether CCP and BST owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their PII;

b. Whether CCP and BST's security measures to protect BST's data systems were reasonable considering best practices recommended by data security experts;

c. Whether CCP and BST's failure to institute adequate protective security measures amounted to negligence;

d. Whether CCP and BST failed to take commercially reasonable steps to safeguard patient PII; and

e. Whether adherence to HIPAA, FTC data security recommendations, and industry standards on data security would have reasonably prevented the Data Breach.

92. Finally, all members of the proposed Class are readily ascertainable. CCP and BST have access to patient names and addresses affected by the Data

Breach. Using this information, Class members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(On behalf of Plaintiff and the Class against CCP and BST)

93. Plaintiff repeats and incorporates by reference the preceding paragraphs.

94. As a condition of receiving health care services, Plaintiff and Class members were obligated to provide CCP their PII.

95. Plaintiff and the Class members entrusted their PII to CCP with the understanding that CCP would safeguard it.

96. CCP had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII were wrongfully disclosed.

97. CCP had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, *inter alia*, designing, maintaining and testing BST's security protocols to ensure that Plaintiff's and Class members' PII in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding patient PII.

98. Further, BST had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, *inter alia*, designing, maintaining and testing its security protocols to ensure that Plaintiff's and Class members' PII in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding patient PII.

99. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures that CCP and BST employed. CCP and BST knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, that they had inadequately trained their employees, and that their security protocols were insufficient to secure the PII of Plaintiff and Class members.

100. CCP and BST's own conduct created a foreseeable risk of harm to Plaintiff and Class members. CCP and BST's misconduct included, but was not limited to, their failure to take the steps to prevent the Data Breach as set forth herein. CCP and BST's misconduct also included their decision that BST would not comply with industry standards for the safekeeping and authorized disclosure of patient PII.

101. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or

practice by businesses, such as CCP and BST, of failing to use reasonable measures to protect PII/PHI. The FTC publications and orders described above also form part of the basis of CCP and BST's duty in this regard.

102. CCP and BST further violated Section 5 of the FTC Act by failing to use reasonable measures to protect patient PII/PHI and not complying with applicable industry standards, as described herein. CCP and BST's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class members.

103. Further, BST violated the Safeguards Rule of the Gramm-Leach-Bliley Act by failing to use reasonable measures to protect patient PII/PHI and not complying with applicable industry standards, as described herein.

104. Plaintiff and the Class members had no ability to protect their PII once they entrusted it to CCP and it gave it to BST.

105. CCP and BST have admitted that Plaintiff's' and the Class members' PII was wrongfully disclosed to cybercriminals as a result of the Data Breach.

106. CCP and BST breached their duty to Plaintiff and the Class by failing to exercise ordinary and reasonable care in protecting and safeguarding their PII while it was within their possession or control.

107. CCP and BST unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of CCP's patients' PII.

108. CCP also unlawfully breached its duty to adequately disclose to Plaintiff and Class members the existence and scope of the Data Breach.

109. But for CCP and BST's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class Members' PII/PHI would not have been compromised.

110. As a result of CCP and BST's negligence, Plaintiff and the Class have suffered and will continue to suffer damages and injury including, but not limited to, out-of-pocket expenses associated with mitigating against the heightened risk of identity theft and fraud caused by the Data Breach; the time and costs associated with remedying identity theft and fraud fairly attributable to the Data Breach; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

111. These harms are directly and proximately caused by the Data Breach.

SECOND CLAIM FOR RELIEF
BREACH OF CONTRACT INCLUDING THE COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Class against CCP)

112. Plaintiff repeats and incorporates by reference the preceding paragraphs.

113. CCP offered to provide medical treatment services to Plaintiff and Class members in exchange for payment.

114. Plaintiff and the Class accepted CCP's offer to provide medical treatment services by paying for and receiving said treatment.

115. CCP required Plaintiff and Class members to provide their PII, including names, dates of birth, particular treatment services and their corresponding codes, billing codes, insurance description, medical record numbers and other clinical and treatment information related to care in order to receive care from CCP.

116. Plaintiff and Class members exchanged valuable consideration – money – with CCP for services, a crucial part of which was CCP's implicit promise to protect their PII from unauthorized disclosure.

117. In its Privacy Policy, CCP expressly promised Plaintiff and the Class that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

118. Necessarily implicit in the agreement between CCP and its patients, including Plaintiff and Class members, was CCP's obligation to use such PII for business and treatment purposes only, to take reasonable steps to secure and safeguard that PII, and not make disclosures of the PII to unauthorized third parties.

119. Further implicit in the agreement, CCP was obligated to provide Plaintiff and the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their PII.

120. Plaintiff and the Class would not have entrusted their PII to CCP in the absence of such agreement with CCP.

121. CCP materially breached the implied contract(s) they had entered with Plaintiff and Class members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. CCP further breached the implied contracts with Plaintiff and Class members by:

a. Failing to properly safeguard and protect Plaintiff's and Class members' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PHI that CCP created, received, maintained and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

122. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of CCP's material breaches of its agreements.

123. Plaintiff and Class members have performed as required under the relevant agreements, or such performance was waived by the conduct of CCP.

124. Under the laws of New York, good faith is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging

performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

125. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

126. CCP failed to promptly advise Plaintiff and the Class of the Data Breach.

127. In these and other ways, CCP violated its duty of good faith and fair dealing.

128. Plaintiff and members of the Class have sustained damages as a result of CCP's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

THIRD CLAIM FOR RELIEF
TRESPASS TO CHATTELS
(On Behalf of Plaintiff and the Class against CCP and BST)

129. Plaintiff repeats and incorporates by reference the preceding paragraphs.

130. Plaintiff and the Class entrusted their PII to CCP with the understanding that it would keep that information confidential. CCP transmitted the PII to BST in the course of engaging its accounting services.

131. CCP and BST intentionally dispossessed the Plaintiff and the putative members of the Class of their PII and/or used or intermeddled with the Plaintiff and the putative members of the Class's possession of their PII, when it allowed cybercriminals to access it, going far beyond the bounds of any consent Plaintiff and the Class bestowed upon CCP and BST.

132. As explained at length above, Plaintiff and the Class members were damaged thereby.

FOURTH CLAIM FOR RELIEF
BAILMENT
(On Behalf of Plaintiff and the Class against CCP)

133. Plaintiff repeats and incorporates by reference the preceding paragraphs.

134. Plaintiff, the Class, and CCP contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to CCP solely for treatment and the payment thereof.

135. Plaintiff's and the Class's PII was transmitted to CCP in trust for a specific purpose (treatment), with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

136. CCP was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and the Class's PII.

137. Plaintiff's and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than the parties intended.

138. As explained at length above, Plaintiff and the Class were damaged thereby.

FIFTH CLAIM FOR RELIEF
NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law § 349 *et seq.*
(On Behalf of Plaintiff and the Class against CCP)

139. Plaintiff repeats and incorporates by reference the preceding paragraphs.

140. New York General Business Law § 349 ("GBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

141. As a large healthcare provider, CCP conducted business, trade or commerce in New York State.

142. In the conduct of its business, trade and commerce, and in furnishing services in New York State, CCP's actions were directed at consumers.

143. In the conduct of their business, trade, and commerce, and in furnishing services in New York State, CCP collected and stored highly personal and private information, including PII belonging to Plaintiff and the members of the Class.

144. In the conduct of their business, trade, and commerce, and in furnishing services in New York State, CCP engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of GBL § 349(a), including but not limited to the following:

a. CCP misrepresented and fraudulently advertised material facts, pertaining to the sale and/or furnishing of healthcare services to the Class by

representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches and cyber-attack, and moreover, that its business associates would do the same;

b. CCP misrepresented material facts, pertaining to the sale and/or furnishing of insurance, health benefits, and other services, to the Class by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to privacy and security of Class Members' PII, and that its business associates would do the same;

c. CCP omitted, suppressed, and concealed the material fact of the inadequacy of its business associate, BST's privacy and security protections for Class Members' PII;

d. CCP engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801);

e. CCP engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Class Members in a prompt

and accurate manner, contrary to the duties imposed by N.Y. Gen Bus. Law § 899-aa(2);

f. CCP engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Class Members' PII from further unauthorized disclosure, release, data breaches, and theft;

145. CCP systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff and members of the Class;

146. CCP willfully engaged in such acts and practices, and knew that it violated GBL § 349 or showed reckless disregard for whether it violated GBL § 349.

147. As a direct and proximate result of CCP's deceptive trade practices, Class Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, and the loss of the benefit of their respective bargains.

148. The above unfair and deceptive practices and acts by CCP were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

149. CCP knew or should have known that BST's computer systems and data security practices were inadequate to safeguard Class Members' PII and that risk of a data breach or cyber-attack was highly likely. CCP's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and

willful, and/or wanton and reckless with respect to the rights of members of the Class.

150. Plaintiff and Class Members seek relief under GBL § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

SIXTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class against CCP)

151. Plaintiff repeats and incorporates by reference the preceding paragraphs.

152. In the alternative to the claims alleged above, Plaintiff alleges that she has no adequate remedy at law and bring this unjust enrichment claim on behalf of the Class Members.

153. Plaintiff and Class Members conferred a monetary benefit on CCP in the form of payment for healthcare services. Plaintiff and Class Members also provided their PII to CCP.

154. The money that Plaintiff and Class Members paid, directly or indirectly, to CCP should have been used by it, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

155. As a result of CCP's conduct described herein, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between healthcare services associated with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and

the inadequate healthcare services without reasonable data privacy and security practices and procedures that they received.

156. Under principles of equity and good conscience, CCP should not be permitted to retain money belonging to Plaintiff and Class Members because CCP failed to use that money to implement the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal and state law, and industry standards and best practices.

157. CCP should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by CCP.

158. A constructive trust should be imposed upon all unlawful or inequitable sums received by CCP traceable to Plaintiff and Class Members.

SEVENTH CLAIM FOR RELIEF
CONVERSION
(On Behalf of Plaintiff and the Class against BST)

159. Plaintiff repeats and incorporates by reference the preceding paragraphs.

160. At all times relevant hereto, Plaintiff and Class Members had ownership rights to their PII.

161. BST engaged in the wrongful act of disposing of the PII by giving cyber criminals access to it.

162. As explained at length above, Plaintiff and the Class were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class as heretofore identified, respectfully pray this Honorable Court for judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representative and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of themselves and the Class, hereby demand a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: June 12, 2020

Respectfully submitted,

/s/ James J. Bilsborrow
James J. Bilsborrow (Bar Roll #519903)
WEITZ & LUXENBERG, P.C.
700 Broadway
New York, New York 10003
Ph: (212) 558-5500
Email: jbilsborrow@weitzlux.com

Samuel Strauss (*pro hac vice* to be filed)
Austin Doan (*pro hac vice* to be filed)
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Email: Sam@turkestrauss.com
Email: AustinD@turkestrauss.com

Lynn A. Toops (*pro hac vice* to be filed)
Lisa M. La Fornara (*pro hac vice* to be filed)
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV (*pro hac vice* to be filed)
Martin F. Schubert (*pro hac vice* to be filed)
Peter J. Jannace (*pro hac vice* to be filed)
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
martys@bsjfirm.com
peterj@bsjfirm.com

Counsel for Plaintiff and the Proposed Class